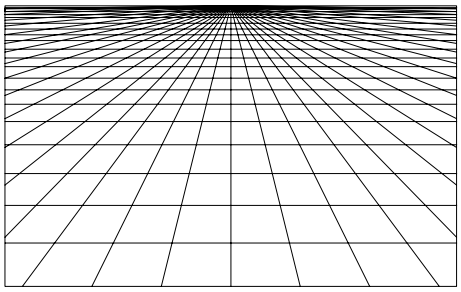
U N I V E R S I T Y O F O S L O

FACULTY OF SOCIAL SCIENCES

TIK

Centre for technology, innovation and culture
P.O. BOX 1108 Blindern
N-0317 OSLO
Norway
http://www.tik.uio.no



ESST
The European Inter-University Association on Society, Science and Technology
http://www.esst.uio.no

The ESST MA

Constructing security – The implementation of the SET technology in Norway

Kjartan Øygarden
University of Oslo/University of East London
The ESST MA/Europe in an information society: Theory and policy
2001

18.785 Words

Synopsis:

This dissertation is focused on the implementation of the SET technology in Norway. This technology is meant to create secure electronic transactions; by many seen has the major obstacle for e-commerce. The dissertation uses the SCOT theory to see how the implementation was conducted and how the different social groups responded to the introduction of this technology. The implementation of the SET technology was unsuccessful, due mainly for the technology's failure to convince the social groups that it could be implemented without major technical difficulty. With this failure, the social groups have turned their attentions to competing technology. This dissertation tries to map some of them, and also tries to give some indication as to how the process might reach its conclusion.

Keywords:
E-commerce, SET, SSL, protocols, Internet, secure transactions, smart cards, PKI

Acknowledgments:

I would very much like to thank the following persons for their help during the writing of this dissertation. My supervisor Anders Ekeland, for his enthusiasm and constructive feedback. My very good friend, Nils Henrik Solum, for his patience and helpful suggestions. Knut Edmund Furu at VISA Norge, Per Aam at DNB, Håkon Røstad at Yatack and Ola Aanstad at BBS for making time in their busy schedules to talk to me. From the Internet community: Kristian Hansen, Tor Andre Breivikås and Tor Rust. Last, but not least, I would like to thank my wife, Siv Hofsvang, for all help and support, both financially, emotionally and intellectually. I could not have done this without her.

Chapter 1. Introduction

1.1 Background

There has been an enormous optimism in the later years for the possibility to exploit the Internet for commerce. The possibilities where regarded as limitless, and investors where eager to invest in this new field. Huge investments were being made, and the DotCom companies was valued in the millions of dollars, even if they have little of the assets, found in more traditional companies, such as real estate, means of production, etc. The year 1997 was expected to be the year that this new channel of commerce directed at private consumers would "take of",[1] and an explosive development were predicted. After the initial euphoria died down, however, it became clear that the road towards generating profit from e-commerce were somewhat longer than expected. Some of the initial attempts went bankrupt in rather spectacular ways; perhaps the biggest one being the Scandinavian company Boxman.com who emerged in 1997, selling CD's over the net. This venture collapsed after three years, having lost a staggering 600 mill NOK.[2] Several more of the initial investments declared bankruptcy as well, the stock markets around the world quickly reacted to this, sending the stocks of Internet-based companies tumbling down. However, there is still an assessment that it will be possible to generate profit with this kind of commerce, but the expectations have become somewhat more sombre and possibly more realistic.

[1] "Dette mener nettproffene", Dagbladet, Helle Høines, 1996

[2] "Tapte på idiotsikker forretning", Nettavisen, 13. July, 2001.

It has been claimed in many reports and surveys that the biggest obstacle to economic growth in e-commerce is security regarding electronic payment. Although there is a claim amongst the expert in the field that it is no more dangerous to use your payment card on the Internet, even without any secure transmission,[3] the customers have not responded in the way investors have hoped. In a recent survey, the Norwegian research institution MMI found that 74% were sceptical or very sceptical to give their account or credit card numbers on the net.[4] In order to deal with this problem, the investors in the field had to convince the market that this kind of commerce was safe. In October 1999 VISA/MasterCard introduced the SET (Secure Electronic Transmission) protocol. This protocol is considered 100% safe; it's by many considered "the flagship"[5] within electronic payment systems. Since this would solve the security problem, one should expect that the protocol would be received with eagerness and its implementation would proceed smoothly. An additional factor that should be expected to influence the introduction of the SET protocol; was at the time of its implementation, the two companies VISA and MasterCard controlled ca 80% of the world market of payment cards.[6] This should also have been an incentive for actors within e-commerce to implement the technology. There is of course the possibility of engaging in e-commerce without the use of electronic payment. By sidestepping the security question, one could use ordinary invoicing as payment method, which are as secure as it can get. However, studies in Norway have shown that the cost of such invoicing is considered high.[7] In

[3] "Sikkerhet og dobbeltmoral", Dagbladet, Tore Neset, 6. February, 1997.

[4] "Internettundersøkelse", MMI AS, Oslo, 2001.

[5] "YaTack først med supersikker netthandel", Aftenposten, 09.June, 2000.

[6] Intervju med Knut Edmund Furu, VISA Norge, 2001

[7] One estimate often cited is 500 NOK for each transaction; cost that the estimates have shown could be reduced to 70 NOK pr transaction by using electronic payment. P. 10, eNorge, Nasjonalt program for elektronisk handel og forretningsdrift med fokus på SMB, Programbeskrivelse, 1. Aug. 2000

other words, it would be very profitable for the commercial interests to introduce a secure system for electronic payment on their web-shop. All in all, there are many incitements for e-commerce to implement a technology like the SET.

However, before I will look more closely on the issues of security, it may be fruitful to consider why security is an issue. In the next sections, I will give a short introduction to the development of the net and how it became a channel for commercial activities. I will also try to show the role of secure technologies in this development.

1.2 A brief introduction to the Internet and how it became a channel for commerce

1.2.1 Early years

When we think of the Internet today, we have a tendency to think of the net as the World Wide Web and the system of e-mail. It is easy to forget that this technology is not a homogenous one, but rather a patchwork of technologies, each developed by different actors as answers to demands of new functionality from the net. The story of the Internet usually starts with a series of memos written by J. C. R. Licklider at MIT in August 1962. In these memos, Licklider introduced a term he called the Galactic Network Concept. The general idea outlined a network that one could connect to almost from anywhere, and which had no limitations in size or content. Mr. Licklider was appointed the first head of the computers section within ARPA (Advanced Research Projects Agency), an agency within the ministry of defence in the USA. ARPA was established to coordinate the research and development needed to bridge the gap between American and Soviet technology after the launch of the Sputnik satellite in 1957. The computer department of the ARPA, an office called

IPTO (Information Processing Techniques Office), was just a small part of the ARPA, receiving around 10% of the total funding.[8] One of the first goals of this office was to think of new ways for the army to use computers in warfare. The main problem of the day was that the computers itself were fast enough, but the full resources weren't used. What slowed it down was that the users would wait until the person using the computer was finished, before initiating their own project. This process would lead to a lot of "dead time" on the computer and Mr. Licklider then suggested ways of "timesharing", where many people could use the machine at the same time. Building on the concept of a galactic network, the idea was to connect computers in vast networks so that all the resources could be pooled. The first two computers where connected to each other, MIT's TX2 and Berkley's Q-32 in 1965, but it soon became clear that the technology available at the time was not adequate for this kind of connection. Attention then was given to something called Packet Switching Theory where software, as opposed to hardware, would translate the stream of data. The packet switching for the Internet works like this: "… messages are divided into packets before they are sent. …Each packet contains the determination address. … Each packet is then transmitted individually and can even follow different routes to its destination."[9] In other words, the information being sent is broken up into small segments, each of them capable of reaching its destination. When the segment gets there, the software of the receiving computer recompiles the segment into the original message. However, this wasn't enough. In the early days of the computer, there were no more standards as there are today. So in order for the different machines to talk together, there must be a common ground on which they

[8] P. 12, "How the web was born", James Gillies & Robert Cailliau, Oxford University press, Oxford, 2000

[9] Source: Webopedia: Online computer dictionary for Internet terms and technical support, www.webopedia.com

can communicate. To solve this problem, the protocol was introduced. There are a variety of different protocols, some are small and easy, other large and complex. But they all have the same function: "An agreed-upon format for transmitting data between two devices."[10] This way, two computers running on different platforms could communicate over a connection. The protocols have also been called "handshaking", because of its similarity to how human interact before the communications starts.[11]

1.2.2 The importance of protocols

Protocols are fundamental for the Internet. Whenever the net has grown, the existing infrastructure very often created a demand for more functionality, and in most of these instances the problems related to this have been solved by the introduction of a new protocol. As the net grew protocols were being either replaced by other, better ones, or new protocols would just take their place alongside old ones. One example of this is the change between the initial network protocols that where used, the NCP (Network Control Protocol), which had a tendency to "clog" the packets being sent. If one of the packets sent, didn't get there, the rest would be useless. This constituted a major problem, and it was critical that this problem was addressed in order to let the net grow and incorporate larger groups of users. The solution to this problem was the TCP/IP (Transmission Control Protocol/Internet Protocol). This protocol not only had the ability to retransmit individual packets that were lost, it also opened up for the Open Architecture that Licklider envisioned in the early 60's, where each network would stand on its own and could connect through the use of the same protocol. This also meant that there would be no global control over the net, so no

[10] Ibid.

[11] P. 4, "How the web was born", James Gillies & Robert Cailliau, Oxford University press, Oxford, 2000

part of the network could (theoretically) shut down or control the rest of the net. The change from NCP to TCP/IP was somewhat of a "D-Day". On January the first 1983, all hosts on the net changed protocol simultaneously. This change was planned for several years, and to everyone's surprise, went smoothly with almost no problems at all.[12]

As we will see in this dissertation, the introduction of the SET and SSL protocols are very similar to this situation. A need for security develops on the net as commercial interests take to the field, and security protocols are developed in order to address this issue. As we also shall see below, it is difficult to force a technology on the net, unless the net itself accepts it and integrates it into its network. The key word for this process is functionality, whether or not the technology introduced meets the requirement, but also if the technology can be easily introduced in the existing infrastructure.

1.2.3 The early users

When considering the growth of the net, it is important to remember that this was still the arena for researchers and computer related people. The net was closed to most people, and indeed still is, if one considers the world as a whole. However, among the researchers it was quickly recognized as a useful tool. It introduced a much faster way of communications between these, and the RFC (Request For Comments) became a popular way of spreading ideas and ongoing work. This was an electronic board where one could post almost anything and ask for other members of the community to pitch in with ideas and comments. Since research is vitally dependent on exchange of ideas, this possibility was a quantum leap in matters of

[12] It gave rise to the button "I survived the TCP/IP transition" though. (A similar experience to the hysteria surrounding the millennium bug on New Years Eve 2000.)

speed and efficiency. By posting an idea or thesis on the electronic board, one could get instant feedback, even without leaving ones office or going to a conference. This also bonded different groups, and the idea of free information available to all interested became one of the cornerstones of the net. This spirit among the pioneers on the net is still very strong in groups on the net today.

As the net grew, more applications where developed by different actors. One of the most popular applications today, the e-mail, was introduced in 1972[13] and made the job of spreading and cooperating on ongoing work easier. The net was still firmly rooted in academia and it would be many years before the e-mail system became available to others than a limited group of researchers. Since its development and use where usually funded and run by learning institutions, there was limited impact on the outside world. Navigating between the few servers available at the time was done with character-based interfaces. These browsers consisted of line of text, which then was navigated with pressing corresponding numbers for the information needed. But with the wide diffusion of personal computers among more regular users in the late 80ties, there was a need for this to change. In order to get more users connected, the level of technological know-how needed for using this technology had to be lowered, so that these new users could participate on the net.

1.2.4 The rise of the World Wide Web

By the late 80's and beginning of the 90's, the personal computer was making its impact in the western world. Around this time a young Taiwanese American developer by the name of Pei Wei was starting his work on a browser that would use

[13] Source: Internet society (ISOC) All about the Internet: A brief history of the Internet, www.isoc.org/internet-history/brief.html

graphical interface, instead of numbers to navigate. Partly inspired by the Mac technology, that used this kind of interface in order to use their machines, Mr. Wei started to develop a browser called Viola (Visually Interactive Object-oriented Language and Application). At the same time, he came into contact with CERN (European Organisation for Nuclear Research) which where starting to spread a Internet system called the World Wide Web. This web used hypertext as a way of navigating, and the combination with the Viola browser proved fruitful. Although the Viola browser introduced many of the features known and used today, such as Bookmark facilities, back/forward buttons, log feature,[14] it still had many shortcomings. These shortcomings where to be addressed when the browser Mosaic was introduced in 1993. With the Mosaic browser, the web became accessible to everyone with a PC or Mac and a modem to connect with. The first year (1994) after the Mosaic was introduced, the web expanded with an enormous rate, outperforming any competing technology by far. The Mosaic browser was developed by NCSA (the National Centre for Supercomputing Applications) at the university of Illinois. The people responsible for the development later left the university, and went in to business for themselves under the name of Netscape Communications Corporation, which at its zenith would reach a 95% market share of Internet-browsers. Internet, and thus the WWW, was now opening up to people outside a small group of connected computer people.

1.2.5 Pioneers of e-commerce

With the net open for the general public, new opportunities arose. One of the first pioneers in trying to use the net for commercial purposes, were the publishers of computer books, O'Reilly and Associates. Having secured the services of Mr. Pei

[14] P. 214, "How the web was born", James Gillies & Robert Cailliau, Oxford University press, Oxford, 2000

Wei, they wanted to be the first publishing house to publish a book electronically. They also launched the website GNN (Global Network Navigator), which was a free Internet-based information centre. This site also included a section where companies could advertise, and soon set the standard for similar resource sites. This site, together with the site for the Lillehammer Olympics, boosted the use of the WWW.[15] The Olympic site also showed what problems could be expected in the future; with the number of hits well over the million mark within two weeks of the games itself. The servers, one in Oslo and a mirror at Sun Microsystems, California, had at some times trouble with coping with all the traffic the site was generating. By 1995, the WWW became the dominant way of using the net, overtaking the most popular program to that date, the FTP (File Transport Protocol) which let you download files to your computer, but not read them before downloading.

Other actors took their first tentative steps into e-commerce also. Pizza Hut, an American company selling pizzas, opened a site where you could place your order online. FirstVirtual Internet bank pioneered banking over the net, but it soon became apparent that these efforts where in vain. In order to facilitate shopping on the net, one need a system of keeping track of what you're buying as you skip back and forth between the pages. A system called "cookies" was introduced. A cookie stores information about what you have been doing on the net.[16] This, however, was not to be the solution. A common complaint at the time was that someone else could use the information stored in the cookies, this including the account numbers of credit cards. The scepticism for this solution grew and soon developers of web-browser had to make it an option if they wanted to continue with the cookie technology or not.

[15] P. 254, Ibid.
[16] P. 259, Ibid.

With this development, Internet approached another critical point. Commercial interests now stood in line for getting their hands on the new technology and the possibilities it offered, but the existing technology did not manage to meet the demand for security of neither industry nor private consumer. The problem had to be fixed, and an obvious solution was to introduce a new protocol.

1.3 E-commerce

Before I introduce the SET technology with its protocols, I would like to give some definitions that would help in narrowing the scope of this dissertation.

1.3.1 Security definition

When considering matters of security, it is easy to forget that a system is only as secure as the lowest denominator. This is, in most cases, the password. There are many examples from the development of security systems that emphasizes this. Stories of complete secure systems where the persons responsible for security, change the user passwords frequently, but still have been successfully “hacked” by outsiders, are quite common. And this is the main point. With this frequent changes of the passwords, another problem surfaces. Many of the users can have difficulties in remembering the password, especially if the password is long and utilizing both letters and numbers. When this is changed frequently, the temptation to write these down would therefore be great and this would, of course, lower the security. The whole-line security will depend on how this password is kept. It is easy to imagine that a 100% secure system would have major flaws if the passwords to enter it with were written on a yellow post-it note, hidden under the keyboard. This is a problem that is beginning to attract attention, and solutions are being sought. Another problem is the fact that on computers using Windows 95 or 98 as platform, there is an option of having the program remembering the password for the user. This would lower

security immensely, because if the computer is hacked, the hacker could very easily read the passwords stored in the memory. For the sake of argument in this dissertation, I will consider the password question solved, i.e. that the passwords are either not written down, or if it is written down, that the user stores it securely and that the memory function in the platforms described above, is not used.

1.3.2 E-commerce definition

Since this is a new field of commerce, there are many different definitions of it. In recent surveys, there is a clear indication that the net is used by many to research for later shopping through more traditional channels. This can be called “Offline-shopping”. Many companies have picked up on this, and put great emphasis on creating homepages with information of their products, even if the company in question does not sell the item itself. This of course, demand little in the way of security. However, there is a growing trend towards making goods available to be ordered and paid over the net. This can be called “Online-shopping”. This dissertation will concern itself with mainly the online-shopping, since the SET technology addresses the security issues raised by this kind of commerce.

1.3.3 Expectations and possibilities

It is still a widespread belief that although there were some problems in the beginning in this new channel of commerce, there is still good prospects of generating profit through e-commerce. The Norwegian government launched its plan for electronic commerce on the first of August 2000, where it stated its expectations and action-plan for this kind of activity: “Trough the eNorway plan the government have as a goal that Norway shall be in the forefront of the development of electronic

commerce and business internationally."[17] The most important goals of this plan are: "Strengthened competition ability, reduced transaction cost and increased turnover."[18] A similar optimism can be found at NHO, Næringslivets hovedorganisasjon (The Confederation of Norwegian Business and Industry). It has registered the later years development, and have a somewhat cautious approach to the subject. In their report "Internett – Steg for steg" (Internet – step by step),[19] they emphasise the possibility of using the net as an information channel for future offline trade. It also underlines the importance of "… finding the right level of ambition…"[20]. It recommends a slow expansion, in order to avoid the mistakes made by early investors who, to some extent, can be said to have over-estimated the consumer's readiness to get involved with e-commerce. The issue of security is not the only issue for e-commerce. In many cases in the past attempts, the goods on offer weren't that much cheaper than in regular stores, and many of the web-shops had great difficulties with their logistics, thus having problems with delivering the goods within a reasonable time, some even failed to deliver at all.

As for the kind of goods, there is quite a diversity that is offered on the net. Ranging from books, CD's, videos, computers to clothes, furniture and even whole kitchen's can be bought on the net. It is obvious, however, that the more standardised a product is, meaning that the product in question is well known and one doesn't have to touch it, test it or try it on, the greater are the possibility of selling it over the net. The most popular item to be sold over the net in Norway are books, which currently stand for

[17] P. 4, Sit: "Gjennom eNorgeplanen har regjeringen som målsetning at Norge skal være i forkant i utvikling av elektronisk handel og forretningsdrift internasjonalt." eNorge, Nasjonalt program for elektronisk handel og forretningsdrift med fokus på SMB, Programbeskrivelse, 1. Aug. 2000

[18] P. 13, Ibid.

[19] "Internett – Steg for steg" (Internet – Step by step) Næringslivets Hovedorganisasjon, Avd. Mindre bedrifter, eierskap og næringsjus, November 2000.

16% of the total sales, followed by Music/CD's with 14% of the market.[21] Both items are very standardised, which might give the buyer less qualms of purchasing on the net, rather than through regular channels.

Although the e-commerce is on the increase, there is still a long way from the scenarios that where predicted in the mid 90thies, only 1,6% of the total private consumption is traded through the e-commerce channel.[22] Only 0,5% of the total turnover in Norway was from this kind of commerce.[23] Studies have shown that security still is the most important impediment to the growth of e-commerce. In addition to scepticism amongst consumers, also commercial actors already established in the field are concerned with security issues, 19% of the firms engaged in e-commerce regard security as their biggest obstacle.[24] The before mentioned NHO report is also concerned with security issues relating to commerce over the net, but it tries to reassure its readers with that the swindle with payment cards didn't arise with the net, but is a problem related to all commerce.[25] However, the report view security as the main barrier towards e-commerce as well, and puts great emphasis on the need for secure transactions systems in order for e-commerce to grow.

---

[20]P. 5, "Internett – Steg for steg" (Internet – Step by step) Næringslivets Hovedorganisasjon, Avd. Mindre bedrifter, eierskap og næringsjus, November 2000.

[21] Global e-commerce report 2001, Taylor Nelson Sofres Interactive, 2001.

[22]P. 7, (Numbers are from October 2000), Rapport nr. 971, "Nordmenns Internettbruk og e-handel", Norwegian Computing Center – Applied research and development, Ingvar Tjøstheim og Ivar Solheim, Oslo, Mars 2001.

[23] P 34, (Estimated for 1999), Bruk av informasjons- og kommunikasjonsteknologi i næringslivet 1999, Geir Martin Pilskog og Erik Sverrbo, Statistisk sentralbyrå, Oslo – Kongsvinger, September 2000

[24]P 33, (Estimated for 1999), Bruk av informasjons- og kommunikasjonsteknologi i næringslivet 1999, Geir Martin Pilskog og Erik Sverrbo, Statistisk sentralbyrå, Oslo – Kongsvinger, September 2000

[25] P. 10, "Internett – Steg for steg" (Internet – Step by step) Næringslivets Hovedorganisasjon, Avd. Mindre bedrifter, eierskap og næringsjus, November 2000.

1.4 Research problem

The main point in this introduction can be summarised as follows: The accessibility of the www that is the very core of the Internet community, not only facilitates speed of information, but also opens a potential for commercial activities. However, the very openness that is the basic for the success of the net, also incurs a risk for the users of commercial services. These risks, whether real or perceived, severely hampers the development of e-commerce. The SET technology is seen as the technological answer to the problems arising from the evolution of the www as a commercial channel described above. Since the SET technology is also presumably cost effective and would install the sense of security so vital to potential customers, one would expect that the diffusion and the use of this technology would be instantaneous and numerous. Yet at the time of writing, only 80 web-shops have implemented the SET protocol, with an additional 130 having signed contracts to implement it in the near future. The question that arises out of these facts, and the one I shall try to answer in this dissertation is this: If the biggest obstacle to economic growth within e-commerce is security regarding electronic payment, why haven't more actors in the field implemented the 100% safe SET protocol, by many regarded as the best technology available?

In order to answer this question, I will make use of the SCOT (Social Construction Of Technology) theory. First I will give a brief introduction to this theory. Then I will start using it, by showing the network and the actors within it. Having established a framework of who the actors are, I will then proceed with an analysis using the SCOT model, before I draw the conclusions.

Chapter 2. Theory and Method

"Invention is a social process, not a psychological one."
-Wiebe E. Bijker

2.1 Introduction

In order to explain the inconsistency between the apparent usefulness and the diffusion of the SET technology, I will focus on the SCOT model. As will be shown, the strength of this model of social construction is that it separates usefulness from the notion of "the best technological solution". In traditional narrations, the technological characteristics are often used as explanation of the success or failures of technological solutions. These results are often explained by the inherent qualities, or lack of these, in the products that are analysed. However, social models also emphasise the roles of actors and networks, as explanatory factors of a products success or failure.

In this chapter I will, after a brief introduction, present the concepts that will be used as an analytic tool in the dissertation. Having done this, I will try to show how I intend to use them.

2.2 The SCOT theory

2.2.1 General introduction

Building on Kuhn's theory of changes in technology and science, the SCOT model tries to explain how technology and science are constructed through networks of social actors. Utilising the idea of paradigm shifts that would explain both change and continuity in technology, the question that SCOT tries to answer is this: who or

what constructs technology? In most cases, an idea of a linear development from initial research, trough testing to finished product, have been the way to explain technological development. In developing a technology, it is constantly under the influences and pressure of different social groups, from researchers, manufacturers, consumers and politicians. If one tries to squeeze these groups into a linear scheme, one can easily see how restraining the linear approach would be. In order to get at all participants in a technological development, one have to abandon the regular linear thought, and approach it with an open mind and be ready to go where the empirically study leads. One of those who have tried to construct a workable theory within this field is the researcher Wiebe E. Bijker. In his book *"Of Bicycles, Bakelite, and Bulbs - Toward a theory of sociotehnical change"*, he uses the SCOT (Social Construction Of Technology) model in order to build a network-theory of technological change. According to Bijker, a theory of technological development must explain four criteria. It must be able to explain both *change and continuity*. "The conceptual framework should allow for an analysis of technical change as well as of technical continuity and stability." It must also contain *Symmetry*. "The conceptual framework should take the "working" of an artefact as *Explanandum,* rather than *Explanans;* the useful functioning of a machine is the result of socio-technical development, not its cause." Further it should explain *Actor and structure.* "The conceptual framework should allow for an analysis of actor-oriented and contingent aspect of technical change as well as of the structurally constrained aspects." And finally, it should view the actors in a *seamless web*. "The conceptual framework should not make a priori distinctions among, for example, the social, the technical, the scientific, and the political."[26]

[26] P. 13, *"Of Bicycles, Bakelite, and Bulbs - Toward a theory of sociotehnical change"*, Wiebe E. Bijker, MIT press, London/Massachusetts, 1995.

2.2.2 Concepts of SCOT

In order to meet these requirements, Bijker introduces certain concepts. The first concept is the one Bijker calls *Artefact*. An artefact is the product or development of the product we chose to study. During the development, the same artefact can achieve many different interpretations and understandings, but when these understandings converge, they will diminish and gradually close in on one interpretation. The SCOT model is very much geared towards empirical studies, and so before the study of the artefact begins in earnest, we need to look for the *prehistory*, an introduction to the times and places of the artefact. The next element is *relevant social groups*. These are groups involved in the development of the artefact. Bijker suggests two ways of doing this. One is "snowballing", a method where one start with looking at the artefact and taking note of all groups involved in the process. As the study goes forth, there will be less and less new groups mentioned, and all groups have been found when no new groups emerge. The other way of identifying the relevant social groups is by asking the members of the social groups to mention who they think all the relevant groups are. After a while no new groups will emerge, and the work is done when no new groups are mentioned.

These groups will have different backgrounds, behaviour and habits. To get these into the picture, Bijker uses the concept of *technological frames*. This is where the group's appropriate responses will have its foundation. The technological frame contains such patterns as goals, problem-solving strategies, current theories, tacit knowledge, testing procedures, design methods and criteria, and also the user's own practice. The SCOT model also emphasises that an individual can belong to more than one technological frame. A person can be an engineer and have that particularly

technological frame, but the same person can also be an investor with a great interest in computer science. At this point one should consider the degree of *inclusion* the person have in the different frames. If the inclusion is strong in the engineer frame, the person will to a large extent manoeuvre within this frame. It is imperative to understand that technological frames change over time, and that a person can bring parts of different frames together. As Bijker puts it: "Existing practice does guide future practice, though without logical determination."[27]

Having established the concepts of different social groups, each with distinct technological frames, we need to go one step further. Each of these groups will have different understanding of an emerging artefact, depending on their frame. Bijker calls this *interpretive flexibility*, meaning that for each of these groups, the artefact will have a different meaning. When an artefact goes trough the process of interpretive flexibility, one groups view tends to gain ground. This process Bijker calls *closure*. As more and more social groups understand the artefact in the same way, the closer to closure one gets, until one interpretation get accepted by all relevant social groups. When closure comes to an end, we get *stabilisation*. After this there will be no more widely differing understandings or interpretations, just a common understanding of the artefact. There is, however, one more concept that needs to be addressed, and that is the notion of *power*. This is what determines the ability of the relevant social groups to impose its interpretation of an artefact on other relevant social groups. These are the main concepts of the SCOT model, and I will now show how I intend to use them.

[27] *"Of Bicycles, Bakelite, and Bulbs - Toward a theory of sociotehnical change"*, Wiebe E. Bijker, MIT press, London/Massachusetts, 1995.

2.3 Method

In short, the model can be summarised in a table.

ARTEFACT: SET			
Social groups	*Technological frames*	*Interpretive flexibility (perceptions of SET)*	*Power*
The developers			
The banks			
The payment solution providers			
The commercial actors			
The users			
The newspapers			

This table will be filled in below. In this dissertation the artefact will be the SET technology. The prehistory of the artefact is outlined in the previous chapter, and the main point is that the SET technology is seen as a solution to security problems that have risen in the development of e-commerce. Regarding social groups, the methods suggested by Bijker is beyond the scope and the timescale of this thesis. Based on preliminary literature studies, I intend to start with the a priori conception that there are six relevant social groups. The groups are, in no particularly order:

1) The developers, represented by VISA Norway. Information from this group have been gathered from an interview with Knut Edmund Furu at VISA and also from their website and other open sources.
2) The banks that provide the private user with the technology, in this case DNB. The information here was from an interview with Per Aam at DNB and also through open sources.
3) The payment solution providers, which in Norway are BBS, represented through an interview with Ola Aanstad and also open sources.

4) The commercial actors, represented by Yatack, the first web-shop in Norway to implement the SET protocol. Represented by an interview with Håkon Røstad and open sources.

5) The users, which will be represented by reports and surveys already done on consumer behaviour and conceptions.

6) The newspapers, represented by articles that have been published on the subject in latter years, forming people's attitude and conception of the security problem.

As for technological frames, I intend to narrow the concept down to two questions: What are the actor's goals? What strategy are they using to achieve these goals? When this is established, I will turn the attention towards how the different actors perceive the SET technology. This will be done, as stated above, through interviews with some of the actors and by accessing surveys/reports/articles already available on the subject. Since the SET technology was introduced quite recently, in October 1999, it might be premature to make claims toward whether or not it has achieved stabilisation and closure. If the conclusion is that it has not reached this stage, I intend to use these concepts to try to see if there are any indications to what might be expected to happen when the process enters this phase. Finally I will use the concept of power to see how the different actors have manoeuvred, knowingly or unknowingly, in order to get their interpretation accepted.

To sum it up, I will use the SCOT model to analyse how the social actors have influenced the introduction of the SET technology in Norway. By identifying these actors, and the processes within which they operate, I intend to present a model of

how the SET technology was implemented and in this way be able to explain the modest diffusion of this technology.

Chapter 3. About SET, the Actors and the Network

3.1 The SET technology

3.1.1 The SET technology – how it works

It is important to understand that the SET technology is supposed to be a part of a larger system. It is meant to be a part of a worldwide infrastructure, a PKI (Public Key Infrastructure), where it would not matter where the customers or sellers were located. Since issues surrounding security is among the foremost of the concerns of all participants in this field, it seems imperative that such a technology gets implemented as soon as possible. As previously stated in this dissertation, the SET protocol is regarded by many as the best of the technologies available. It was developed by VISA and MasterCard, with advice and assistance from such companies as IBM, Microsoft, Netscape and VeriSign amongst others. The development of the technology started in 1995, as a response to a situation where both VISA and MasterCard where developing similar, but not coordinated systems. Since the owner structure of both companies are very similar, both being owned by much of the same international and national banks, it was decided that it would be a good idea to pool the resources and develop one standard. After testing and pilot projects, it was introduced and certified in Norway in October 1999. The SET technology has been published as a detailed public specification, so that other software vendors might use it to produce application with the SET protocol as the

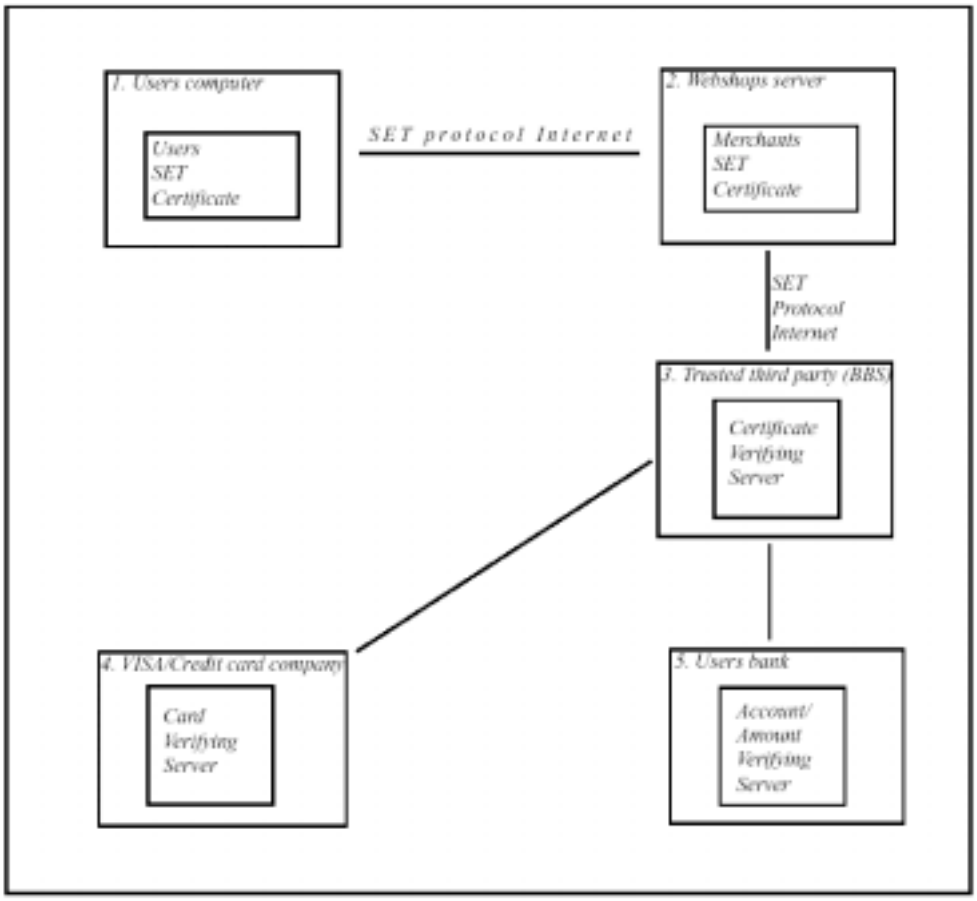
basic technology. The SET was supposed to addresses several major business requirements: [28]

1) "Provide confidentiality of payment information and enable confidentiality of order information that is transmitted along with the payment information." This in order to deal with the greatest fear among the actors, that the card details of the buyer gets hacked into and misused by other persons.
2) "Ensure the integrity of all transmitted data." So that none of the parties involved can alter any of the data without the consent of the other participant.
3) "Provide authentication that a cardholder is a legitimate user of a branded payment card account." This is the focal point that the SET technology tries to address, that the user of the card is the same as the owner. This is done through certificates that the customer would be issued with.
4) "Provide authentication that a merchant can accept branded payment card transactions through its relationship with an acquiring financial institution." Not only the customer needs these certificates. To attain full security the merchants also need to be certified. This in order to prevent a false website to obtain payment.
5) "Facilitate and encourage interoperability among software and network providers." Interoperability is also high on the priority list for the developers. In order to get this system to work, it is

[28] P. 6, Book 1: Business description, SET Secure Electronic Transaction Specification, Version 1.0, May 31 1997, VISA/MasterCard.

important that other payment cards can be used as well as different computer systems.

Figure 1: How the SET technology is supposed to work



In order to meet these requirements, the SET protocol functions like this: Before anything can happen, the customer that wants to use this technology, must approach his/hers card issuing bank. In Norway, there were two banks that offered this service, Den Norske Bank and Sparebanken Hedmark. The customer applies for the SET program, which is then sent on a CD-rom to the customer's home, or downloads the program directly from the net. The program, when installed, will make a virtual pocketbook on the PC, which then will be used for transactions. Before any transactions can take place, however, the user will have to download his/hers certificates from the issuer or another issuing party. This could be the issuers of the

card itself, or an independent registration authority,[29] a trusted third party catering for multiple card brands that can forward the request to the proper issuer. In Norway this is BBS (Bankenes Betalings Sentral) who fills this function. The certificates are created with the use of complex cryptography, and the SET protocol use dual signatures.[30] These certificates will be used to confirm that the user is really the person it claims to be. "Cardholder certificates function as an electronic representation of the payment card. Because they are digitally signed by a financial institution, they cannot be altered by a third party and can only be generated by a financial institution."[31] Also of some importance and interest is that these certificates does not give the account number when used for electronic shopping, it only assures the merchant that the card is authentic. Whereas it is the banks in Norway that are responsible of distributing the SET protocol among their customers, VISA Norway have taken the responsibility of signing up the merchants. VISA Norway signs the deal for licensing the technology, but the merchant must buy the programs necessary for instalment from another company, the BBS. The merchants would also have to implement the SET protocol together with the corresponding certificates. "Merchant certificates function as an electronic substitute for the brand decal that appears in the store window – the decal itself is a representation that the merchant has a relationship with a financial institution allowing it to accept the payment card brand."[32] The merchant would need a certificate for each card brand he/she accepts. This certificate is also provided by BBS, as it is for the private consumer. The role of BBS and other participants will be discussed in the next chapter. With all the certificates in order,

[29] P. 34, Ibid.

[30] One signature that is located within the SET application on the users PC, and one that follows the transaction.

[31] P. 25, Book 1: Business description, SET Secure Electronic Transaction Specification, Version 1.0, May 31 1997, VISA/MasterCard.

[32] P. 25, Ibid.

the transaction on the net will be in fact safer than traditional use. This because the merchant does not at any point in the transaction see the users card numbers, and therefore reduces the chances of fraud. If one is to use a payment card in a regular shop, the shop will get access to your card number, and it opens up the possibility of fraud, not only from the shop itself, but also if the recite is found by others. With the SET, this possibility disappears.

3.1.2 How to use the SET technology

An example: Lets imagine that a customer was to buy some goods from the company Yatack. After the customer finish browsing on the shop and have decided on an item that he/she wish to purchase, he/she goes to the virtual cash register, and choose the SET protocol as method of payment. Yatack then sends a demand (wake up call) to his/hers computer. It activates the virtual pocketbook and the person confirms that the sum of the demand is what he/she should pay for the goods. After this confirmation, the person will be asked to type in his/hers password. The password is far longer than the pin codes used for regular transactions, consisting of between 8 to 16 characters, using both numbers and letters. (This is close to impossible to break, but the security here will depend on how this password is stored. See definition above.) When the password is confirmed (by the software on the persons computer), it will then sign the demand with an electronic signature/certificate and the transaction goes back to Yatack. Yatack now have to sign the transaction with their electronic signature, before the transaction can be sent to the Payment Solution Provider (in Norway, BBS). The payment solution provider then checks both certificates, and confirms that they are valid. If one or both certificates were found to be invalid, the transaction would not be completed. Also, if the amount that the person authorised to be withdrawn from the account has been changed, the

transaction would be invalid. The reason for this being that the amount the person is to pay is encrypted within a message digest that follow the certificates, thus making it impossible for the seller to alter the sum after the signing. After this check, the payment solution provider sends the transaction to VISA, in order to see that the card is valid and that the agreement is in order. After this has been cleared, the transaction is sent to the person's bank, to check that he/she has the amount available. If there is enough money for the transaction, the sum will be reserved on the account, and a message will be sent to Yatack who then can deliver the goods ordered. The reason for the amount to be reserved, and not paid directly to Yatack at this point, has to do with Norwegian law that prohibits anyone to take payment before the goods are shipped unless other has been agreed amongst the participants. (Delivered here means sent from the shop.) When the goods are sent, Yatack send a payment demand with the transaction code from the reservation and payment is then completed. The transaction code can only be used once, and thus making repeated or fraudulent claims impossible. The transaction have now been completed, and the person should (hopefully) get his/hers goods in a couple of days, Yatack have got its payment, and there is no chance for anyone to see the credit card details during the transmission of the data.

3.2 The actors

It is time to take a look at what have been done with the SET technology in Norway. But in order to do that, we need to take a closer look at the groups and actors that have been involved in this process. It is very important to keep in mind that when the SCOT model introduces what it calls "Relevant social groups", we shift our viewpoint from that of an outside observer to that of them-selves. What might seem troublesome and difficult for an outsider, might be regarded as straightforward and

easy by that group. The group in question also might not have the same information that the observer has, and therefore might have a different perception of the events and developments of the technology. I will first give an introduction to the different actors, with a quick prehistory, so that we can better understand their actions in the network.

3.2.1 The developers – VISA

VISA is the worlds leading payment system. They take care of almost half of all the card transactions in the world, and can be used in 22,4 million places worldwide.[33] The story of VISA starts in 1958 when Bank of America introduces its payment card in California. In 1974 the company IBANCO Ltd. was started in order to develop a system to use the cards internationally. In 1976 IBANCO changed name to VISA and their responsible for the copyright, product development and operating the system for all VISA products. VISA is a member organisation for 21.000 banks worldwide, and has a staggering 1 billion cardholders.[34] VISA Norway was established in 1977 and is owned by Norwegian business- and savings banks. At present time, there is 2,8 million cards in Norway with an average turnover of 75.000 NOK pr card, which put Norway in the top of the world regarding card use.[35] (Its important to note that the VISA card in Norway is a debit card, not a credit card as it in the USA.) VISA International, together with MasterCard, is the developer of the SET technology. As stated above, it was a cooperative effort, drawing on the resources of many big companies such as IBM, Microsoft, etc. It was developed in order to address the problems regarding the use of credit cards on the Internet, a payment method that was gaining popularity at the time. Although there where

[33] Source: Visa Norway's, homepages, www.visa.no/visa/presse/historikk/.
[34] Ibid.

testing in the period before, the SET was officially introduced in Norway in October 1999 by VISA Norway.[36] VISA Norway is responsible for the SET technology in Norway. The main focus has been on introducing it to commercial actors within e-commerce, making the implementation possible on the web sites. They do, however, not sell the software necessary for the implementation; this is done by the Payment solution provider, which in Norway is BBS. At the present time, 85 web-shops have implemented the protocol, with another 130 customers having signed agreements to do so in the near future.[37] VISA International expects to have 17 – 18.000 web-shops up and running with the SET technology by the first of October 2001.[38]

3.2.2 The SET solution providers – BBS

The BBS (Bankenes Betalings Sentral) was established in 1972 and has a similar owner structure as VISA Norway.[39] It is owned by the business- and savings banks of Norway, and its purpose is to provide payment services to Norwegian banks. These consist of three main fields of expertise, namely card-, giro- and interbank systems. When it comes to SET, BBS stands as the Payment Solution Provider in Norway, i.e. the deliverer of the software needed by the web-shops to implement SET. This is software BBS have bought from Globeset, a company specializing in making this kind of systems. The company, originally from Ireland, offers software that incorporates both SSL (Secure Socket Layer) and SET. BBS got involved with the SET technology 4 – 5 years ago, when they participated in a pilot project called "Trygg netthandel" (safe net shopping), a cooperation between banks in Norway, BBS, the card companies and some selected private web-shop companies. BBS

[35] Ibid.
[36] Interview with Knut Edmund Furu, at VISA Norway, 8. August 2001.
[37] Ibid.
[38] Ibid.
[39] P 13, BBS årsrapport 2000 (annual report),

ambition was to help develop a PKI (Public Key Infrastructure) for electronic payment in Norway.[40] BBS regards the use of payment cards on the net as safe, with the exceptions of when used on adult oriented web sites.

3.2.3 The commercial users of the technology – Yatack

Yatack gets its name from the Norwegian phrase "Ja Takk", meaning yes please. It was the first commercial user to implement the SET technology in Norway, in October 2000. Before this, Yatack.com had been involved in a pilot project, then under the name of online-club. According to Håkon Røstad, the IT-manager at Yatack, this pilot project failed due to problems with getting the pc-wallets to work. They felt, however, that it was important to present them selves with the best security available. Yatack doesn't necessarily agree with the notion that security is the only issue for successful e-commerce. Largely based on their own experiences, Yatack believes that other issues, including customer relations and delivery time, are of equal importance. Addressing these issues continuously, Yatack have the ambition of being the leading web-shop in Scandinavia.

3.2.4 The provider for private SET users – DNB

DNB (Den Norske Bank) is the largest business bank in Norway, controlling approximately 30% of the market. It is also the largest issuer of payment cards, having ca 900.000 cards on the market. The bank issues VISA, MasterCard and American Express cards. DNB was the first to introduce the SET technology to private customers. They bought the software from the Danish company PBS (Pengeinstitutternes Betalings Systemer), a company with many of the same functions and structures as the Norwegian BBS. This software was developed by

[40] Interview with Ola Aanstad, at BBS, 17. August 2001.

PBS in cooperation with IBM, and DNB chose this software in order to avoid any interoperability problems, thus trying to join an existing infrastructure. However, DNB has a strong interest regarding e-commerce and have recently created the company called Doorstep.no, a joint venture with the Norwegian telecommunications company Telenor, which will cater for user-friendly solutions for e-commerce, including payment solutions.[41] It is interesting to note that this company will utilise and offer all available technologies within this field.

3.2.5 The private users of the technology – The customers

It can be said that this group is the focal point of the network. This because it is the group that all other actors are working to get involved with e-commerce as potential customers. It is estimated that 63% of the Norwegian population have access to the Internet, from either home or work.[42] Out of these, 30% have shopped on the Internet at least once in 2000, tree times as many as at the same time in 1998.[43] As mentioned, the users are sceptical of the use of payment cards on the net.[44] There are many other reasons given for not wanting to shop on the net as well, such as fear of lower quality of goods, many find it too difficult, others doubt that the web-shop can deliver within reasonable time and the yet others find it more fun to buy goods in a regular shop. However, the fear of security related issues are by far the most important reason for customers to abstain from shopping on the net. From this, we can draw the conclusion that a majority of the users regard the net as unsafe, and therefore are reluctant to engage in e-commerce.

---

[41] P. 9, DNB Årsberettning 2000 (Annual report)

[42] P. 10, table 1, (Numbers are from November 2000), Rapport nr. 971, ”Nordmenns Internettbruk og e-handel”, Norwegian Computing Center – Applied research and development, Ingvar Tjøstheim og Ivar Solheim, Oslo, Mars 2001.

[43] P 11, Ibid.

[44] “Internettundersøkelse”, MMI AS, Oslo, 2001.

3.2.6 The reporters of the technology – The press

This is another group of great diversity. Norway is among the nations that read the most newspapers in the world even if it is mostly local papers, making the task of whom to choose to represent this group a difficult one. However, I have chosen the tree largest newspapers in order to represent this group.[45] The reason for this is that these papers are read by a very large part of the population, and thus have a larger impact on the population. While more specialised papers, like Computerworld, are more precise in their reporting on e-commerce, they have less impact due to lower circulation. VG and Dagbladet are so-called boulevard presses and are sold mainly over the counter while Aftenposten rely on subscription to sell their newspapers. This would tend to affect how the different newspapers present their news, with the boulevard press tending to go for the more spectacular headlines in order to attract customers. All newspapers take a great interest in the Internet, reflecting Norwegian population use of the net. All three newspapers have established web-versions of their papers in print, Dagbladet have currently started offering its customers to read the whole printed newspaper on the net, charging payment over the mobile phone. (The paper would then be downloaded in an Acrobat reader format, to be printed or read on the screen.) Most of the news coverage related to the security issue concerns themselves with the Internet and the dangers lurking there. The headlines in the two boulevard papers have a tendency to go for the spectacular, rather than the accurate.

The general attitude towards the SET technology in the media is that it is safe, but as will be seen below, this seems to drown in the horror stories describing what awaits a careless user on the net. Although the press is very differentiated in their way of

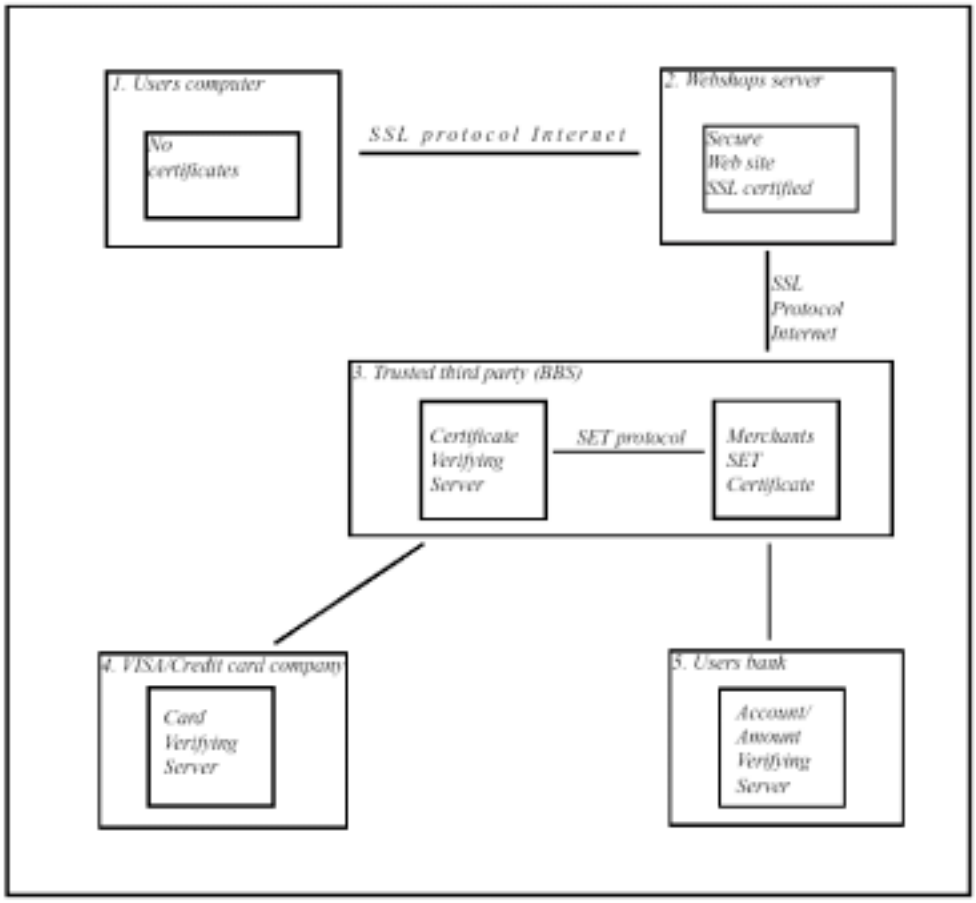
[45] The largest the three are VG (Verdens Gang) claim to have 1.4 million readers on a weekday, while Dagbladet and Aftenposten claim 824.000 and 781.000 respectively.

reporting on this subject, the main focus is still on “negative” reporting, playing on readers fears and thus create an impression of an insecure Internet, safe payment technologies or not.

3.3 The network - How is the SET technology actually working?

It became quite clear to me, in the early parts of the information gathering, that the SET technology did not function as it was intended. For a quick recapitulation of how it was supposed to work: VISA developed this technology, and is responsible of signing up commercial user who will then buy the software needed from BBS, in order to implement the SET technology. BBS will then, as payment solution provider, hand out the certificates needed and also provide a server where these certificates would be authenticated. The banks in Norway cater for the private customers, providing these with the corresponding certificates and the software needed. With all infrastructure, software and certificates in place, the users would then have a guarantee that only they could use their cards on the Internet, and that the web-shop would not have access to the card details. This has not happened.

Figure 2: How the BBS ePay works



The first problem occurred when the technology was made available to the private users by DNB in Norway. With very little focus on marketing and even less emphasis on technical support, the interest for the SET technology dwindled almost immediately. The SET software was offered to DNB's Saga gold customers, a group of customers considered to be very important to DNB, in February/March of 1998. The response, however, was disappointing. As was the response when DNB offered it to the other private customers. Almost none of the private users implemented it, according to DNB, because of few places to use the technology. BBS, who sold the software to the commercial users had to take this into account, and created a hybrid SET solution called ePay, that used SSL encryption on the user level, instead of the SET protocol. This meant that although the card is protected against outsiders trying to get access to card details through hacking over the net, there is no guarantee that

the user of the card is the same as the owner of the card. And indeed, in Sweden Yatack have experienced fraud with people using stolen cards, ordering goods on their web-shop. However, there was no difficulty in tracking these criminals, since the goods where in most cases sent to their home addresses. But the problem with this was that the goods where sent, and usually sold by the criminals, while Yatack was left to cover the bill for the fraud.[46] With the authentication process for the user gone, most of the intended function of the SET technology is gone as well. To further complicate matters, the commercial users complained that the software sold by BBS was to complicated to be installed on their local servers, opting for a solution where the certificates in question was to be stored on the servers at BBS.[47] This however, meant that also the security level between the shops and BBS fell away, replacing the SET protocol once again with the SSL encryption,[48] further reducing the SET infrastructure. So BBS electronically signs the transactions on behalf of the commercial actors, after the web-shops have sent the information to BBS. The SET technology is still used though, between to servers residing one meter apart of each other, in a basement at BBS. The servers are not connected to each other through the Internet, making the SET technology here totally redundant. It is a standing joke at BBS that this is the most secure transaction in the world, since any attempt to hack it would require the hacker to be physically present in the basement. There is little or no chance for the SSL encryption to be hacked into during the transactions over the Internet, but the problem with both user authentication and of visible credit card details still remain, and it was these issues SET was supposed to address.

[46] Interview with Håkon Røstad, Yatack, 15 August, 2001.
[47] Interview with Ola Aanstad, at BBS, 17. August 2001.
[48] 4.4, BBS ePay, Implementeringsguide, versjon 1.4, 2001.

As for the other side of security, with the users being subjected to fraudulent behaviour from web-shops, there are very little actual chance of this to happen, since all participant in this network have signed contracts regulating this field to such an extent that fraud would maybe not be impossible, but at the least very easily discovered. A problem would of course rise if a website was genuinely false, with fraud as its only purpose. However, it would be very difficult for the creators of this site to get away with the crime, considering the electronic trail that would follow such a scheme.

3.4 SET, actors and their interactions

3.4.1 The implementation of the SET technology

According to VISA, SET came to a slow start in Norway; partly because it was launched just before the turn of the new century when everybody was busy with the expected Y2K problem, therefore maybe not to eager to install other software at that moment. Also VISA didn't put to much emphasis on advertising, feeling that this would draw resources away from the implementation process itself. The SET standard is marketed with pages on the VISA.no website, with links to banks and to web-shops which have implemented the technology. VISA feels that the e-commerce is on the verge of taking off, and that we only have seen the start of things yet to come. Another explanation for the slow expanse of the SET technology is that VISA feels that the banks have been a little slow on picking up on the private customers side. VISA see this as a "chicken and the egg" problem, where the banks where reluctant to push SET to their customers because there were few web-shops you could use it on, while the web-shops were reluctant because so few potential customers have implemented it. VISA however, now feel that they have created a

market for where the technology can be used, and that it is time for the banks to "come to the playing field",[49] i.e. start implementing the SET for its private customers. For VISA Norway, the SET technology is unproblematic. It is the only certified trademark within this field today, and it is regarded by VISA as close to 100% secure one can get. Since the security level is so high, VISA Norway offers something called liability shift, to the customers who implement it on their web-shop. This liability shift moves the responsibility for fraud from the web-shop to the bank. The way VISA sees this, is that if the web-shop have implemented the SET protocol, they have done their part and are therefore not responsible for any fraudulent behaviour that might occur. This responsibility falls to the banks in Norway, who would have to cover the web-shop's losses and also have the job of finding out what have happened. Its important to note that this liability shift occurs even if the customer in question is not using the SET technology when making payment. As for security without the SET technology, VISA Norway believes that a customer is reasonably secure when trading with known trademarks, like when a customer is booking a flight at SAS's (Scandinavian Air Service) website. The largest amount of complaints of fraud on the Internet is, according to VISA Norway, related to sites containing gambling and pornography. Still according to VISA, this might have several reasons including where the customer have not read the agreement for the particular site, and therefore have agreed to continuous billing. Other methods might be false websites, which can be found within the same fields, which lure their prey in by claiming that giving their credit card details is only regarded as proof of age, and will not be misused. VISA also believes that some of the people claiming to have been swindled on the net have actually been aware of

[49] "… komme på banen…." Interview with Knut Edmund Furu, at VISA Norway, 8. August 2001

their actions, but might feel to embarrassed to admit to watching pornography on the net, when complaining to VISA about fraud.

3.4.2 The response from BBS

BBS, on their side, see more problems regarding the SET technology than VISA does. Since very few private customers had implemented the SET protocol, the web-shops complained of little use. BBS also reckons that the technology is to difficult for the private user to install, especially considering the variety of pc's brands, Mac's and other machines on the market. For instance, there was no version of the SET technology available if the computer runs on Linux software. Also BBS felt that the system of getting the software from one source and the certificates from another was confusing, and that the average user would find this too difficult. The web-shops also complained that the technology was too difficult to supervise and maintain on their servers. At the same time there was a certain degree of anxiousness surrounding e-commerce in Norway. The overly optimistic predictions of profit were proving wrong and it was a need for a secure payment system that the commercial actors felt could change this situation. In order to address this problem, BBS decided to simplify things by dropping the customer part of the SET technology, instead developing a hybrid software that would use both SSL and SET encryption. This solution is called BBS ePay. Although somewhat sceptical to the SET technology, BBS still believe strongly in the possibility of an international PKI, but not necessarily with the SET technology. Together with the banks in Norway, they are currently looking into the possibilities offered by bankID, an electronic signature that could be used as valid verification for both business and consumer activities. They believe that the intention of SET where good, and the technology itself is safe, but

that the applications based on the technology is too difficult for the users to gain widespread implementation.

3.4.3 Incentives for implementing ePay

One of the major factors in Yatack's decision making process when considering secure payment, were the liability shift that moved the cost of fraud from Yatack to the banks, together with the lower commission paid when implementing the BBS ePay solution. The ePay software was bought from BBS, considered by Yatack as the best available. Other software vendors were tried, but found to be more unreliable than BBS's system. After some initial problems with this software, including a somewhat curious bug that prevented Yatack from getting payment if the sum could be divided with 256, the system now seem to have got rid of its children deceases. One of the problems that still haven't been solved is related to payment information. For Yatack it is important to see who makes a payment into their account, so this can be controlled against the customers account. Apparently this information has a tendency to disappear in the system today, but the problem is being worked on continuously. Although Yatack have implemented the SET protocol, it is never used by any customers. Instead they are using the hybrid system developed by BBS (described over), which involves the use of SSL encryption. After the implementation of this technology, the use of credit cards rose from 25% of the transactions, to 50% of the transactions.[50] However, according to Mr. Røstad, the use of credit cards has gone somewhat down after they introduced the option of paying by invoice. As for the security question, Yatack doesn't necessary agree that this is the major obstacle for e-commerce. They regard the security issue as minor compared to the problems regarding delivery and communication with the customer.

[50] P. 4, Yatack Årsrapport 2000 (Annual report),

In the beginning of this venture, there where major problems regarding delivery of goods and with responding to customer enquiries. There is much focus on these two issues within the company, and after changes in routine, the delivery time is now reduced from 8 to 5 days. 90% of customer emails are answered within 24 hours. Yatack believes that their present security solution is "safe enough",[51] but when asked about the SET technology responded that it would not take off until VISA and the banks tell everybody to use it.

3.4.4 DNB's response

In an interview with Per Aam at DNB, he claims that the reason for this lack of interest in the SET technology from the customers is related to the fact that VISA had not provided enough web-shops where they could use the technology. With nowhere to use the technology, the customers couldn't be bothered to implement it. Only what Aam described as techno-freaks where interested in this technology. After the gold-customers had been offered the technology, the offer went to the regular customers. However, there was no active marketing of the SET technology, the information had to be sought at the DNB's website. The software needed could be ordered on a CD-rom in the beginning, which also contained the newest browser available to ensure that the programs technical requirements where met. After a while, the SET software could be downloaded directly from the DNB's server to the home computer. This was a slightly modified product, which had addressed some of the initial problems. But there were not only problems due to lack of interest from the customers. The software itself was problematic to install for the average customer. Some of the problems relate to the lack of standardisation of their PC's, thus making the program difficult to implement. This was the main reason for DNB

[51] Interview with Håkon Røstad, Yatack, 15 August, 2001.

to ship updated web-browsers with the software, but this didn't solve all the problems. The other major obstacle for implementation was that the certificates had to be downloaded from the PBS server in Denmark. According to Aam, there were some problems with this server at the time, making it difficult to download the certificates, and thus adding to the frustration of the customers. Also, there were no official helpdesk at DNB, having to rely on the technicians working on DNB's Internet bank for help. After the SET technology was made available for downloading, only ca 400 applied for it, while ca 50% of them implemented it on their PC's. However, DNB believes that the problems with implementation together with the problem of few web-shops on which their customers could use the technology where to blame for the SET not to take off. And due to these problems DNB decided to quit this project in April 2001. A part of that story is DNB's reluctance to invest heavy in a technology that might be replaced by the possibilities offered by competing technology. The technology that gets the most focus at DNB at the moment is the smart card. DNB feels that this technology would solve all the problems that the SET tried to address, and a few more as well.

3.4.5 The users response

There is a high degree of uncertainty among the Internet users in Norway. This scepticism is in spite of the fact that most experts on the field consider that there are very little chances of card details being misused on the net, especially when dealing with known trademarks. According to Per Aam at DNB, there has not been a single incident where someone has successfully hacked into a transaction, at least not in Norway. Misuse by other means, i.e. fraudulent behaviour by a web-site is not a matter of security technology, but rather a question of carelessness by the card holder, giving card details to less than reputable and honest websites, most often

dedicated to pornography or gambling.[52] In other words, it is a matter of conception of security on the net, rather than the actual security. In a survey from Norsk Gallup Institutt, they measured the knowledge of the SET technology from November 1998 to November 1999. The survey indicated a negative trend in knowledge, starting of at 22% of the Internet users having heard about SET in 1998, sinking to 19% in November1999, one month after the SET technology was officially introduced.[53] (At this point Gallup gave up measuring the SET technology, and instead started measuring N-safe, the Norwegian quality trademark for e-commerce.) Of all who had shopped on the Internet, only 29% used their credit card as payment method in 2000, corresponding nicely with the reluctance to use credit cards on the net. However, in spite of these numbers, Norway is among the nations that shop the most on the Internet. At least 19% of the Internet users have shopped on the net in the last month, placing Norway 4th in the world together with South Korea.[54] (The global average is 15%) Another 23% plan to shop within the next 6 months, although 25% of these prospective have shopped in the last 6 months.[55] Although numbers are on the rise, the sums involved are still small. In a survey from the SSB (Statistisk Sentral Byrå – Statistics Norway) the estimate is that the total turnover for e-commerce is 6 billion NOK, 0,5% of the total turnover in 1999.[56] Estimates from NR (Norsk Regnesentral) for the year 2000, place the total turnover to 9,17 billion, ca 1,6% of the total, indicating a sharp increase in e-commerce.[57]

---

[52] Interview with Per Aam, DNB, 9. August, 2001.

[53] ”Kunnskap om SET/N-safe”, Norsk Gallup Institutt, Taylor, Nelson, Sofres, 2001

[54] P. 23, Global e-commerce report 2001, Taylor Nelson Sofres Interactive, 2001.

[55] P. 30, Ibid.

[56] P 34, Bruk av informasjons- og kommunikasjonsteknologi i næringslivet 1999, Geir Martin Pilskog og Erik Sverrbo, Statistisk sentralbyrå, Oslo – Kongsvinger, September 2000. Note that the banking and finance is exempted from this number, since this sector doesn’t use the term ”turnover”.

[57] P. 35, (Numbers are from November 2000), Rapport nr. 971, ”Nordmenns Internettbruk og e-handel”, Norwegian Computing Center – Applied research and development, Ingvar Tjøstheim og Ivar Solheim, Oslo, Mars 2001.

3.4.6 Reporting on security issues

In Dagbladet's article "Safe as the Bank", the reporter describes the security for electronic transactions are "relatively bad" and that this is the "Dirty little secret" of this sector.[58] The report was on print 9 months after the introduction of the SET technology. In a report 4 days later, under a headline entitled "How you can be affected"; the newspaper described the dangers of the net, listing e-banking and e-commerce together with virus attacks and (cyber) burglary. The very same day a headline read: "(Hackers) Take control of your PC", listing how hackers can break into your computer, claiming that up to 10% of the computers on the net where under hacker control.[59] (They did this by scanning for open ports, i.e. looking for machines that could be opened from the outside by the use of programs known as Trojan Horses. However, they used the word "might be" in the actual report when describing how many of the machines that was under the direct control of hackers.) In spite of the headlines, the reports went on to say that there had been no complaints to the authorities that handle fraud on the net. The newspaper VG use much of the same angle when reporting on e-commerce and the Internet. With headlines such as "They're coming to get you!" and "The road to net-fraud is short"[60] the papers give a perception of the net as a place of lurking danger. The first report is a stern warning against what the hackers and cyber-vandals can do to your machine on the net, and gives advice as to how this can be avoided. The second headline plays on the Norwegian word "Kort", which can both mean short and card. Here VG warns in the ingress that your card can be misused on the Internet, even if you yourself have never used it on the net. Later in the report it concludes that the card details is usually

[58] "Sikker som banken", Dagbladet, 13. July, 2000

[59] "Slik kan du bli rammet", "Tar kontrollen over din PC", Dagbladet, 17. July, 2000

[60] "Nå kommer de og tar deg!", VG, 1. August, 2001, and "Veien til nett-svindel er kort", VG, 17. February, 1999.

stolen or acquired through theft in everyday life, and that the chances of swindle are "infinitively small, but the chances have increased with the Internet."[61] On a more sombre note is the reporting in Aftenposten, by many regarded as the best newspaper of the three. A newspaper that has its biggest sales through subscription, its formats are different. Where the first two are tabloids, Aftenposten are in a larger format, with more text and less pictures. This opens for longer reports on phenomenon such as the Internet. Headlines tend to be less sensational and more to the point, such as "Yatack first with super safe net shopping" and "Not completely safe, but safe enough"[62] thus giving a somewhat different picture of potential danger. Aftenposten also reports on hacking, but the focus is more on how commercial companies are threatened and how they respond to this threat, like the headline "Internet banks could be hacked".[63] In this report, Aftenposten claims that 6 out of 78 largest Norwegian companies could be hacked, three of them Internet banks. However, already in the ingress, the paper reassures the reader that the account information was safe; it was the web pages that could have been tampered with.

In all fairness, it must be said that the newspapers took their cue from the banks and the card companies when they started to report on e-commerce. In an article from Dagbladet from early 1997, the journalist attacks what he sees as a double standard on the behalf of the card companies, where they advice their users not to use their cards on the net, at the same time as the web-shops advertised with payment through known brand names.[64] This attitude from the card companies might be related to the

[61] "Veien til nett-svindel er kort", VG, 17. February, 1999.

[62] "yatack først med supersikker netthandel", Aftenposten, 9. June, 2000, "Ikke helt sikkert, men sikkert nok", Aftenposten, 13. November, 1999

[63] "Nettbanker kunne hackes", Aftenposten, 6. March, 2001.

[64] "Sikkerhet og dobbeltmoral", Dagbladet, 6. February, 1997.

fact that it was they that had to cover the expenses related to fraud at this time. After the liability shift (putting the responsibility for this on the banks) introduced with the implementation of the SET technology, this attitude seems to have changed somewhat. All three newspapers have also reported on the introduction of the SET protocol, reassuring the readers that this technology is the safest to use, but this information might have been drowned in the warnings that at least the two tabloids presents. Aftenposten have also reported on this fact, quoting a survey from PriceWaterhouseCoopers, where user fears are linked to the media blitz of how insecure the Internet is.[65] This survey also makes the point that the different actors have been not good enough in communicating the aspect of safety to the media and population as such.

[65] "Nordmenn stoler ikke på nettet", Aftenposten, 9. December, 2000.

Chapter 4. Analysing SET in a SCOT perspective

4.1 Introduction

I have now shown how the network functions and how the different actors responded to the SET technology when it was introduced. Below, I intend to analyse the empirical data gathered, trying to explain why the different actors responded how they did.

4.2 What went wrong?

4.2.1 A giant with feet of clay?

VISA is the largest payment card company in the world. Involved in more than half of the world's card transactions, they both have extensive experience and knowledge of building payment systems. It could therefore be seen as natural that when a new channel of commerce opens, VISA would be in the avant-garde of addressing the problems that would arise. VISA's goal would then be to create a sustainable system for payment using cards on the net, and the SET technology is their way of achieving this goal. When it comes to power, VISA's size comes into play. By simply being the largest payment card system in the world, the system favoured by VISA could very easily become the standard of the world. If VISA insists on the SET technology, it could be very difficult for any of the other actors to introduce another competing system. However, VISA does also have a weakness, and that is their structure of ownership. VISA, both international and national, are owned by the banks. Although they're organization is free of everyday control of the board, it is still the board of directors who deicide on which direction VISA should go. And the banks in Norway

are very sceptical for the moment, thus making it difficult for VISA to force the SET technology through.

4.2.2 A matter of practicality

A very similar owner structure can be found at BBS. It is also owned by the banks in Norway, and it also has the responsibility of creating systems of payment. With extensive experiences of both manual and electronic payment services, it was natural for BBS to take it upon them the role of payment solution provider and trusted third party. Their stated goal is to provide secure and efficient systems of payment and they are doing this by using any technology available. When BBS felt that the SET technology didn't work, they simply modified it by introducing another technology, the SSL encryption. Thus they created a working technology where the SET technology is only a small part and is a far cry from what VISA intended when they introduced it in 1999. The power-base for BBS is their hands on experience of creating functioning systems for payment, systems that is being used with other forms of payment today. It is an outspoken goal to become the leading company in Scandinavia in this field, competing with similar companies in the other Nordic countries. BBS introduced its hybrid SET version already in November 1999,[66] effectively ignoring VISA's attempt to create a SET infrastructure. Here we see a failure of VISA to force its interpretation of the SET technology on BBS. BBS decided that it wouldn't work, and promptly changed it, leaving VISA sidelined in the process. It must be said that although the technology is a hybrid between several technologies, VISA is still negotiating contracts with e-commercial businesses as if the SET technology was implemented as intended.

[66] Interview with Ola Aanstad, Product manager BBS e-commerce, at BBS, 17. August 2001.

4.2.3 Less trouble, more money

Part of the reasons behind BBS decision to drop part of the SET technology was due to the response from the commercial actors. Yatack is the largest Norwegian web-shop and have been so for quite some time. In order to achieve this position, there were several requirements that needed to be met. Catering for private consumers, almost all of these are related to customer services. In order to sustain their position as Norway's leading e-commerce company, the customers had to be assured that they get the goods for a good price, that the goods are indeed delivered accordingly, questions and responses are met within a reasonable time and that the method of payment is secure and unproblematic. The strategy of Yatack is therefore to be in the forefront of all these requirements. It is therefore in their interest that not only internal routines are continuously being revised, but also that the external parts, like electronic payment is the best available. And this is where this group's power comes in. By stating that the SET technology is to difficult for them to implement on their local servers, the commercial interests forced BBS to create another solution, the ePay system.

4.2.4 The waiting game

The banks also played a big part in forcing VISA's hand. DNB is the largest business bank in Norway, providing services for both commercial and private customers. They make their profit from this, and it is in their interest that these customers have the best offers within all fields of banking, electronic or more traditional. One of the methods the banks use for generating profit is by charging for services. Whenever a person is using his/hers card, in traditional ways or on the Internet, the bank will charge a small fee. Therefore it is in the banks interest to offer services relating to e-commerce. Especially since the method of paying with cards eliminates more

troublesome, and therefore less profitable methods, such as regular billing and invoicing. Security has always played a big part in the banks existence. With slack security, the risk of loosing money becomes greater, scaring both potential and existing customers. By introducing the SET technology to its private customers, DNB hoped to address the new security situation that had opened with the rise of e-commerce. But they're experiences echoes those that BBS got from the commercial actors, the SET technology were considered to difficult to implement. It must be said that DNB didn't go out of their way to make it work either. With almost no resources being allocated for the creation of a helpdesk, the customers were to a certain degree left to fend for them selves, perhaps making the installation of the necessary software to high a wall to climb for regular users. And this is where DNB exercised its power, when they killed the project in April 2001. With this decision, the SET infrastructure lost its most important factor, namely the idea of user authentication. However, VISA has introduced the liability shift, where the banks are responsible of covering losses caused by fraud on the net. This can be seen as a way of forcing the banks, and in this particularly case DNB, to rethink its decision of not offering the SET technology to its customers. But it seems that this is to no avail, and as we shall see below, the banks have already begun to look elsewhere for other solutions that are being developed.

4.2.5 To shop, or not to shop

It is perhaps a bit pretentious to try to see the Internet users in Norway as a single group, which then can be ascribed goals and strategies. Consisting of everything from computer-nerds to pensioners and children, one should watch one's step carefully to not overreach the explanation. However, there are several common goals that can be said to exist. Every user are interested in shopping, online or more

traditionally, without the fear of fraud. If this were said to be the goal, then the strategy would be to choose a safe way of shopping or not shop at all. And this is this group's power. If the internet users simply refuse to use their cards on the net, it will be very difficult for the other actors to introduce a safe technology unless they can convince this group of the merits of such. If the consumers refuse to shop, e-commerce comes to an end. However, Norway being one of the nations with the highest percentage of Internet users, we are to a certain degree interested in shopping on the net. This could be because it is conceived cheaper or easier to shop on the net, or because a person lives in a part of the country that has few shops of a specific kind. Whatever the reason, online shopping is on the rise in Norway, and with it the need for a secure way of making payment. Only parts of the Internet users in Norway where given the choice or opportunity to implement the SET technology, but this groups response was more or less unanimous. The users simply refused to use it, whether it was because of lack of web-shops to use the technology on, or because it was too difficult to implement without help from the bank, its difficult to say. But when DNB's private customers decided against the implementation of the SET technology, they used the user social groups power to stop any further implementation of SET. This move could possibly be countered, but only if the software and installation could be simplified. And as we have seen, the banks have little interest in doing so. The choice of the users to not implement SET, also again affected the choices made by BBS, with no customers using the SET technology, another solution for these had to be introduced. The ePay technology, with SSL encryption, gained further ground.

4.2.6 Danger galore

Another group of great diversity is the press. But yet again, it is possible to see that they have some goals in common. The main goal is to generate profit for its owners through selling news. Another goal, although recent development in the news business seems to contradict this, is to present the news as accurate as possible. But the three newspaper presented in this dissertation differ when it comes to strategy. The different sales strategy of the papers would, of course, greatly affect how they present their news. The tabloids that are sold on a day-to-day basis would then have to use headlines that would attract potential buyers, often competing with other papers on sale. Subscription papers usually don't have to take this competition into consideration, because the paper is already sold before it goes to press. This would account for Aftenposten's apparent more fact oriented reporting, while the two other papers follow the old press idiom that there are no news that a plane landed, but it is "big" news if it crashed. Following this line of thought we can draw the conclusion that the tabloids report with a more sensationalistic approach, with more emphasis on "negative" or "sensational" reporting rather than just factual. It could also be fruitful to ask whether the reporters them selves know the technology in question. One might find it easy to assume that they do, but in the interviews with both VISA and DNB, the representatives stated that there had been no great use of marketing for the SET technology, which could lead to an impression that the press might suffer from a lack of information on the subject. This is also the conclusion in a recent report from PricewaterhouseCoopers, that the reason for much of the uncertainness among the public is related to a combination of negative press reporting and also that the commercial actors have failed to communicate the safety issues properly.[67]

[67] Source: Europeisk Internett undersøkelse, PricewaterhouseCoopers, Norway, homepages, www.pricewaterhousecoopers.com/no/nor/ins-sol/publ/pm_111200_2.html

4.2.7 Closure and stabilization

Now we have seen how the different social groups interpret or understand the technology. And at this point we need to consider the concepts of Closure and Stabilization. Closure is that process an artefact goes through in order to be fully understood in the same way by all social groups, leading to a point where the artefact stabilized and understood in the same way, with no differing interpretation. Of importance to the process of closure is the use of power during the interpreting of the artefact. The SET infrastructure as it was intended, is still in an immature state. The technology itself is being reconsidered at this very moment, thus opening for other interpretations in the future. But for the intended introduction of the SET technology, it has for now ended in a failure. And here is where we see the social construction of technology in action. When VISA Norway introduced the SET protocol, it was presented as a detailed public specification, making it possible for software vendors to use it in making applications for both commercial and private consumers. It was considered as close to 100% secure as any technology could get. BBS began developing software for the commercial actors while DNB bought their software from another vendor, IBM, and remodelled it for use in Norway. But both intended customers rejected the technology, claiming it was too difficult to implement. Now, instead of using their power to force this technology through, both DNB and BBS chose the opposite. Instead of developing more sophisticated software, more adapted to the different technological demands, they closed down their projects. Rather than creating an environment with extensive customer support and helpdesks, these two actors instead to a certain degree scrapped the whole technology. DNB did this totally, by discontinuing their SET project, BBS partially by introducing a hybrid technology with another encryption technology, the SSL protocol. These two actors

were therefore forced by the private and commercial user groups to view the SET technology as inadequate. The introducers of the technology, VISA Norway, could now not implement the intended SET infrastructure because of this. VISA can be said to have tried to use their power in order to secure the implementation, by introducing the liability shift. This made it attractive for the commercial users to implement it, but only the hybrid version and only because of lesser commission paid pr transaction and that the responsibility for fraud would be placed at the banks, and not at themselves as before. This move by VISA could be seen as an attempt to force the banks to reconsider the SET technology. But as of yet, fraud is not a major problem for e-commerce in Norway, therefore it is more cost efficient for the banks to not implement the SET technology. Only if the cost of implementing SET becomes lower than the cost of reimbursing fraud in e-commerce, could this move by VISA succeed. Even then SET could fail, because of competing technology. The banks take a great interest in the possibilities offered by the smart card, a technology the banks feel would solve all the problems attempted to solve by SET, and quite a few more. (This technology will be discussed in a chapter of its own.) This technology and its infrastructure is planned to be in place by 1 January 2005, therefore the banks might be reluctant to invest to much in a technology that they fear might be obsolete in a few years anyway. If we are to consider the concepts of closure and stabilisation on the status of SET as of today, I think it is safe to conclude that the first attempt to implement the SET technology is a failure. It has failed to get accepted by the most vital social groups, namely the private and commercial users, thus making implementation close to impossible. It even fails to stabilize as safe/unsafe, because the question at hand discusses problems related to

installation, rather than security. And if we follow the SCOT model, this would mean that the technology as a whole, for the time being, is a failure.

4.3 Summing up

We have now gathered enough information to fill in the table presented above.

ARTEFACT: SET			
Social groups	Technological frames	*interpretive flexibility (perceptions of SET)*	Power
The developers	To create and service secure payment, by introducing new technological solutions	Technological excellence, solves security problems	Can use the 86% market share of payment cards to force the other actors to accept SET
The banks	To generate profit through services to its customers, by offering secure solutions	Technological demands to high for average users, do not want to commit to technology if cheaper competing technology can solve problems in near future	Can chose other security solutions, instead of SET
The payment solution providers	To create and service secure payment, by introducing new technological solutions	Technological demands to high for average users, Cross platform incompability	Introduce other security solutions than SET
The commercial actors	To create profit through e-commerce, by offering goods and guarantying secure payment	Technological demands to high for commercial users, economic factors determins choice	Can chose other security solutions than SET
The users	To shop without the fear of fraud, through new or traditional channels	Technological demands to high for average users	Can chose not to engage in e-commerce at all
The newspapers	To create profit from , through subscription or regular sales	Internet is unsafe, litle reporting on SET as safe	Can influence potential users conception of e-commerce as unsafe, making SET safety irrelevant

We now see how the different social groups interpret the SET technology, and it is very interesting to see that four of these groups consider the technological demands to high for average users. When this is the conclusion for the majority of relevant social groups, there chances is that a different technology would be developed to address the issues that the SET technology was meant to handle. This would mean that competing technologies would influence the actors' choices within this network. Although this is discussed within the concept of closure, it could be fruitful to

introduce another theory in order to investigate this further. In the next sections I will consider different technologies that could compete with SET. In order to do that, I will use the theory of technological lock in and path dependency.

4.4 Technological lock in/out and path dependency

4.4.1 Introduction

Another aspect of the evolution of SET is competing technologies. Due to what is known as lock in effects, the importance of being successful is an important trait in itself. Before I study how competing technologies impact on the fate of SET, I will briefly present the lock in effect and describe the characteristics of these technologies.

4.4.2 The QWERTY lock in

There are other ways of considering the SET technology. One of the more interesting theories of the later years is Paul S. David's theory of technological Lock in/out. In an article in American economic review[68] I will consider this theory as already known by the reader, but for those who feel for a quick read-up on the theory, should read appendix 1.

4.4.3 SET and technological lock in/out

Now lets see how this theory relates to the SET technology. It was the intension of VISA to build a PKI with the SET protocol at its centre. This technology has been lauded as the best available, and should therefore be in a good position to challenge for hegemony. It was launched at the same time as the SSL protocol by VeriSign, one of its main competitors. The problem however, as we have seen earlier, is that

[68] "Clio and the economics of QWERTY", Paul A. David, nr. 2, (Vol 75), American economic review, 1985.

the SET technology, because of reasons mentioned above, have had problems with getting acceptance and widespread use. The different actors in the field in Norway are simply not adopting it. Norway is a bit late to implement this kind of technology. If one turns to Denmark, it becomes clearer how the competition has developed. The Danish company PBS, which have much of the same functions as the Norwegian BBS, offer two different models of e-commerce security, one based on the SSL technology, the other with SET technology. BBS only offers one solution, the hybrid between SSL and SET technology. This solution has, or is in the process of, been implemented on 215 web-shops. If one turns to Denmark, a total of 2.134 web-shops have signed contracts to do this. However, the SSL technology is being implemented in 2.049 of the contracts, leaving the SET technology with only 85. This could signify a major rate of adoption by the actors in the field in Denmark, which might lock the SSL technology in. The same can be said of the process in Norway. I would therefore make the claim that the critical technology in this system is the SSL technology, simply because it is the one that is actually used to secure the transmission over the net. Also speaking in favour of continuing adoption of the SSL technology is the ease of use. No certificates needs to be downloaded, no troublesome installing of software is needed. The SSL protocol will provide encryption without any hassle for potential customers, thus making it attractive to all users. I create some scenarios in the next chapter, where I will try to give an indication of what might happen with several competing technologies. Also I will show how the intentions of a “user authentication PKI” might give a certain degree of path dependency in the future.

4.5 The rise of competing technologies

4.5.1 E-invoicing

This contender are probably the least troublesome to implement for the ordinary user. They demand very little in investment of infrastructure, the reason for this being that they can be used directly on the existing Internet infrastructure. The only demand for this technology is that the customer has created net access (through Internet-banking) to their account, and that he/she signs an agreement for this new technology. The technology of e-invoicing can be divided into two different ones, E-giro and E-faktura. The similarities in use are so strong that I for sake of argument will treat them as one. E-invoice is the electronic equivalent of its paper counterpart. It is used as one would use a regular giro to make payments to other actors, but will reduce the cost normally connected to this kind of transactions. The customers, especially in the private sector, can use this technology together with other accounting systems that would reduce the need for human interaction. This would of course make enormous savings for the company implementing it. Another factor that counts in favour of this technology is the fact that it has a backup tool ready. If the system should crash or become unstable for some reason, it would be easy for the actors involved to switch back to the old system of paper invoicing. Almost all banks in Norway are now offering this technology to its customers, with BBS delivering the software. On matters of security e-invoice use a system of dual encrypted signatures, not unlike the SET technology, making it easy to spot fraudulent invoices from real ones. BBS will again be trusted third party, verifying that both certificates are valid before completing payment.

Its functionality is very simple; instead of receiving a paper invoice through regular mail, the e-invoice system allows you to get this through the Internet. It is offered through the banks in Norway, and demands that the user have already established an Internet-bank account. Once this is done, the customer can view his/hers bills in the electronic bank, making payment just like one would when using traditional methods. It is important to understand that this system demands that the customer informs the businesses that he/she wants to receive e-invoice from, of where to send the bill. Once this has been done, billing can start, whether it is on a regular basis or just a one-time occurrence. Its appeal is its ease of use, there will be little or no need for the customer to punch long strings of numbers, neither account numbers or identification, since the bill arrives ready to be paid. This system can also be very interesting for e-commerce, since it provides the opportunity to make secure and fast payment without the use of cards. When it comes to security, there are no need for any extra investment, since the Internet-banks already provides ample security for the user.[69] Lets see how this could work out in a scenario.

4.5.2 E-commerce with e-invoice

The introduction of the e-faktura could solve many of the problems that e-commerce struggles with today. It would reduce the cost of the transactions, and also it would eliminate the possibility of fraud with cards. This because there would be easy to check that the person ordering the goods are the same as the one owning the account in the bank. Since a survey have indicated that 95% of the net-bank users could be interested in implementing the e-faktura system,[70] the possibilities of potential customers would rise accordingly. One can easily imagine that the threshold for

[69] The Internet banks usually use a code-generating calculator accessed with a pin code in order to enters ones account on the Internet.

shopping on the net would be lower if a known and trusted technology was used as method of payment. This would solve many of the problems for the e-commerce on a national level. However, there are some problems that need to be solved before this can be used in an international level. One of the ideas of e-commerce is its mobility, the possibility of shopping across borders. For this system to happen on an international level, there would have to be a very strong standardisation of the e-invoicing. One example of this is how this system developed in Sweden, where the three largest banks introduced different systems, not one of them compatible with the others.[71] This meant that if a customer changed banks, he/she would not only have to inform their connections of this, but these companies would then have to implement the other system in order to get continuous payment. In other words, for this technology to work as an international standard, all systems would have to be compatible and implemented by all actors interested in participating in the network

4.5.3 The smart card

One of the competing technologies mentioned most by the actors in the interviews, were the smart card. Especially two of the actors, DNB and BBS, were very interested in this technology, thinking that it would solve all of the problems tried addressed by the SET technology.[72] Countries such as Singapore have already implemented some of these possibilities offered by this technology, introducing cash cards, replacing coins and bank notes for daily purposes. The cost efficiency of this

[70] Source: BBS, homepages, www.bbsas.no/efaktura/efaktura_bedrifter.htm

[71] "Klikk og betal på nettet", Computerworld, 29. March, 2000.

[72] The smart cards technology goes a long way back, all the way to 1974, when a self-taught inventor by the name of Roland Moreno introduced an "electronic stored value application", i.e. a chip based storage device, which he curiously placed in a ring to be worn on the users finger. The idea was to use the ring as a wallet, transferring funds to it when needed, acting as a wallet. It became very clear that this application wasn't as practical as should be hoped, especially considering the size of the ring. Shortly after the demonstration of the rings possibilities, the chip technology was mounted on a flat card. By 1979 the cards where being tested by many French banks, who took a great interest in the possibilities offered by the technology.

is apparent. By using electronic payment, the handling of the transfer can be done automatically, reducing the cost of manual routines. However, the possibilities don't stop with this. In USA the cards have been used to store medical records for the owner, giving medical personnel direct access to the medical history of the patient. It is used in the GMS system for mobile phones, enhancing security and user friendliness. It is used as tickets when travelling by air, booking rental cars and hotels. There seem to be no limit to what the card can be used for. The reason for the interest of DNB and BBS comes down to security and interoperability. Interoperability means that the card can be used and recognized by most, if not all, technological systems in the world. Another factor that speaks in the favour of the smart card technology is that it will have multiple functions, enabling it to be used in more than one field. But the interest for me in this dissertation is to see how it can be used as a device for authentication, thus competing with the SET technology.

Let us see what impact the smart card technology can have on the authentication/payment PKI that is being tried to implement. The basic need for this kind of infrastructure was authentication, thus reducing the chances of fraud. The smart card, together with the pin code, will take care of this problem. However, the smart card requires hardware to work, a smart card reader. In other words, the card can't be used before everyone, or most, of the users have installed this hardware on their personal computers. The smart card is supposed to replace the magnetic strip cards of today by 1 of January 2005. By this time, the problem of whom shall pick up the bill for this upgrade need to be solved. The banks are of course eager to try to make the hardware vendors introduce this technology as a standard for the future personal computers, thus making future customers pay for this themselves. The

reason for this is quite obvious; in Norway there are 1.7 million households. If we say that these households all have a computer, they would all need a card reader in order to use the smart card as authentication. Smart card reader's hardware cost between 150 and 400 NOK in today's prices, the quality reflecting the prices.[73] If we say that the price for high quality hardware drops to ca. 250 NOK because of the sheer bulk of customers, we end up with this equation: 1.700.000 X 250 NOK = 425.000.000 NOK. This is of course a large amount of money, and there is no wonder that the banks are eager to push the bill on someone else. However, in the following scenarios I will assume that the card reading technology is in place, at home or elsewhere, and instead focus on the possibilities of the smart card PKI.

4.5.4 Smart card scenario one – SSL technology

The first scenario deals with the possibility that the SSL protocol have been locked in, and totally dominates the market. This because its ease of use, not requiring any active participation from the consumers, other than using web-shops equipped with it. The SSL encryption is 128 bits, and therefore considered close to impossible to break. (At least not with the computing power of today, and a long time into the future.) The smart cards function in this infrastructure as an authentication certificate. The certificate is placed within the microchip itself, and is accessed through the pin code for the card. This would take care of the problem related to authentication. The smart card would also be a part of a much larger infrastructure, being used as a payment card, credit card, storing information ranging from medical records to CV's and personal information. The mass of information stored in the chip is of course depended on the size of the chip; today a smart card is capable of containing 100 times more information than the magnetic counterpart. With this infrastructure we

[73] Interview with Ola Aanstad, Product manager BBS e-commerce, at BBS, 17. August 2001.

have solved the problem of authentication, but also another problem; the problem related to multiple pin codes and passwords. On the last count, I had 5 pin codes (of which I can remember two) related to various payment-, credit- and security-cards. In this scenario we have dealt with all of these problems. I can now sign documents electronically, buy goods on the Internet as easily and secure as in a regular shop, send my medical or personal information to anyone who then can be assured that I indeed am the person I claim to be. All this, with the use of only one pin code. As for the security for the smart card itself, it offers a great more security than the magnet strip cards used today. This because the magnet strip cards are read only, and can be read by outsiders with the right hardware. Once the card has been read, the pin code will be known and the card can be misused. With the chip technology in the smart card, this becomes if not impossible, then at least more difficult. Since the chip enables the possibility that the card can have different access restrictions, there are more security options. Some parts of the chip can be open to all, for instance blood type and other information needed in a medical emergency. Other part can only be accessed through the use of the pin code, while other parts again are only accessible by trusted third parties only, for instance an electronic purse that only can be reloaded by the issuer bank. This means that a magnetic strip reader can't read the whole card and the pin code will then be very difficult to get, and also the card itself could have the function to shut itself down after three attempts to log on.

4.5.5 Smart card scenario two – SET technology

The second scenario is very similar to the first one. There is a certain degree of path dependency here, which will be discussed directly after the second scenario. In the second scenario we have a situation where VISA flexes its powers. Since VISA controls ca 60% of the world market for credit- and payment cards, and MasterCard

an additional 26%, this gives them a unique position. When the smart card is being introduced, it will replace our existing cards. Since ca 86% of these cards will be VISA or MasterCard cards, all VISA have to do is to insist on the authentication certificates being VISA's own, the SET technology. This again would mean that the SET technology would take the place of the SSL technology, forcing the other actors in the field to comply with this standard. And this is why we should not close the book in the SET technology as of yet. With the SET technology being constantly developed, a future version of it might actually succeed in establishing the network it tried to with the first implementation.

There are of course more underlying premises for these two scenarios. One of them is the idea of a centralized system that will act as a confirmer of the authentications, a trusted third party. This could be the bank of the customer, but most likely an independent third party like the Norwegian BBS, which will be online at all time. With the establishing of such a PKI, all existing payment systems would merge in to one, with its obvious advantages. And this is where the concept of path dependency enters. When the regular magnetic credit- and payment-card where introduced, a PKI with confirming third parties were developed. There is a general understanding in the field, that a PKI for the new channel of commerce have to be established. With both the SSL and SET technology established in the field, and with trusted third parties established with earlier technology, it would be a higher investment cost for any actor to start with another technology. This could mean that most new actors would go for the solution with lesser initial investment. We have also seen that there is an increasing return to the SSL technology, already threatening to lock out competing technology. The cost of a new infrastructure would therefore be too high, and the

chances of a latecomer's challenge are therefore small. I think therefore that it is safe to conclude that the existing PKI will stake the course for future technological solutions, and therefore the development process will be path dependent of the infrastructure that is being established.

Chapter 5. Conclusion

5.1 Summing up

SET solves the technological problems related to security problems in commercial activities (transfer of payment) on the Internet. Thus, the reason for the narrow diffusion of this technology had to be sought elsewhere. Through the use of SCOT I have identified social groups that have had an impact on the fate of SET. While the developers claimed that the SET technology was both safe and unproblematic, the other actors turned it down, because the technological demands were too high. Also the potential private customers, has a general fear of fraud that was fed to a large extent, not by any "real" understanding of the technology involved, but by the general concerns voiced by the mass media. Especially the tabloid versions were over-simplified and based on unrealistic generalisations of the phenomena of credit card, fraud, not the safety of the e-commerce itself. Thus the relevant social groups used their interpretive flexibility based on different technological frames to conclude that the SET technology was inadequate for its task, and sought other solutions elsewhere. This is a process that has yet to come to a conclusion, but I have tried to give some pointers to where this could be headed. As we have seen, the SSL technology has seized a large market share, which could lead to a situation of technological lock in. We have also seen that some of the actors, DNB and BBS, have turned their attention towards the smart card technology, which could be used to establish an international PKI together with the SSL technology. We have also seen that VISA tries to counter this by developing the server-wallet, which is meant to simplify the SET technology. This could make a challenge to the diffusion of the

SSL technology, especially if VISA and MasterCard decided to use their power of their market share of payment cards.

This process will come to a conclusion eventually, and as we have seen, there will be a certain degree of path dependency that will determine how the intended PKI is established. Key words here were interoperability and cost efficiency towards building on an existing network or to introduce a new. The conclusion drawn was that it would be too high a cost to start with a new infrastructure, and that the existing would have to be taken as a starting point for future development.

5.2 Topics for future research

There are several questions being raised by this dissertation that could be interesting to examine in the future. First among them is the question of why the developers of the SET technology made the choices that they did. In today's "mobile" world that puts more and more emphasis on mobility, they developed a system that demanded that the users where stationary on one computer. This is currently being revised, as the developers at VISA are now designing a server-wallet to replace the pc-wallet. The question that rises from this is: Why didn't they develop the server-wallet in the first place? The development of the SET technology was done in USA, with testing throughout the world. At some point, the shift in the demand for such a technology must have asserted itself, and it could be very interesting to make a further study as to when this happened and what conclusions where drawn from it.

Also related to this is the demand for an international Public Key Infrastructure that would enable secure electronic payment. My thesis touches many of the different aspects of this, but several other technologies have been left out. The focus in this

thesis has been on secure protocols, enabling commerce over the net. Since the possibilities offered by this PKI, addresses not only commercial issues but also gives the promise of a digital lifestyle, where digital signatures replacing traditional ones, etc., it has attracted interest from governments around the world, seeing it as a locomotive for economic growth. It could be very interesting to see how the different governments approach this field. Although the Norwegian government take a great interest in what happens in the field of e-commerce, I was somewhat surprised at finding little or no connection to them during the work on this thesis. A further study could therefore be focused on how the government tries, or should try, to regulate and stimulate this sector. There can be no doubt that the field of e-commerce have a lot to gain with an active participation from the government, setting standards for the infrastructure and creating models for “how-to-do” business in this field. With proper regulation, e-commerce gives the promise of cost reduction within both production and administration, removing geographical handicaps and strengthened competition ability.

Bibliography

Bijker, Wiebe E., *Of bicycles, Bakelites, and Bulbs - Toward a theory of sociotechnical change*, MIT press, London/Massachusetts, 1995.

Gillies, James & Cailliau, Robert, *How the web was born*, Oxford University press, Oxford, 2000

Arthur, W. Brian, *Competing technologies, increasing returns, and lock in by historical events*, Nr.99, The economic journal, March 1989.

David, Paul A., *Clio and the economics of QWERTY*, nr. 2, (Vol 75), American economic review, 1985.

Nærings og handels departementet, *eNorge, Nasjonalt program for elektronisk handel og forretningsdrift med fokus på SMB*, Programbeskrivelse, Aug. 2000, Norway.

Næringslivets Hovedorganisasjon, *Internett – Steg for steg*, (Internet – Step by step), Avd. Mindre bedrifter, eierskap og næringsjus, November 2000.

Tjøstheim, Ingvar & Solheim, Ivar, *Rapport nr. 971 Nordmenns Internettbruk og e-handel*, NR, Norwegian Computing Center – Applied research and development, Mars 2001, Oslo, Norway.

Pilskog, Geir Martin & Sverrbo, Erik, *Bruk av informasjons- og kommunikasjonsteknologi i næringslivet 1999*, Statistisk sentralbyrå, Oslo – Kongsvinger, September 2000, Norway.

Eilertsen, Rune, *Internettundersøkelse*, MMI AS, Oslo, 2001.

Taylor Nelson Sofres Interactive, *Global e-commerce report 2001*, 2001.

Kunnskap om SET/N-safe, Norsk Gallup Institutt, Taylor, Nelson, Sofres, 2001

PricewaterhouseCoopers, *Europeisk Internett undersøkelse*, Norway, homepages, www.pricewaterhousecoopers.com/no

Newspapers:

www.dagbladet.no, *Dette mener nettproffene*, Høines, Helle, 1996, *Sikkerhet og dobbeltmoral*, Neset, Tore, 6. February, 1997, *Sikker som banken*, Elvik, Halvor13. July, 2000, *Slik kan du bli rammet, Tar kontrollen over din PC*, Sarastuen, Kristian & Bore, Bjørn K., 17. July, 2000

www.vg.no, *Nå kommer de og tar deg!*, Olsen, Rune Fjeld, 1. August, 2001, *Veien til nett-svindel er kort*, Buggeland, Svein A., 17. February, 1999.

www.aftenposten.no, *Ikke helt sikkert, men sikkert nok*, Valvik, Marita E., 13. November, 1999, *yatack først med supersikker netthandel*, 9. June, 2000, *Nordmenn stoler ikke på nettet*, Gimmestad, Johnny, 9. December, 2000, *Nettbanker kunne hackes*, Haugnes, Gunhild M., 6. March, 2001.

www.nettavisen.no, *Tapte på idiotsikker forretning*, Heftøy, Jens Egil,13. July, 2001

www.computerworld.no, *Klikk og betal på nettet*, Bakken, Jonas Blich, 29. March, 2000.

Web resources:

Internet society (ISOC), *All about the Internet: A brief history of the Internet*, www.isoc.org

Webopedia: Online computer dictionary for Internet terms and technical support, www.webopedia.com

BBS homepages, www.bbs.no.

DNB homepages, www.dnb.no.

VISA homepages, www.visa.no

Yatack homepages, www.yatack.no

Annual reports:

Yatack Årsrapport 2000 (Annual report)

DNB Årsrapport 2000 (Annual report)

BBS årsrapport 2000 (annual report)

Technical descriptions:

Book 1: Business description, SET Secure Electronic Transaction Specification, Version 1.0, May 31 1997, VISA/MasterCard.

4.4, BBS ePay, Implementeringsguide, versjon 1.4, 2001.

Appendix A

A.1 Qwerty

Mr. David discuss the development of the keyboard used by typing machines and later our computers. The system is commonly known as “QWERTY”, after the first 6 letters from the top left of your keyboard. It competed in its time with, among others, a system known as DSK (the Dvorak Simplified Keyboard), which was by many regarded as superior and more efficient than the QWERTY. In fact, most tests showed that the DSK system could be used with 20 – 40% more efficiency in touch writing, and it holds most of the world’s records for speed typing. Even so, the QWERTY system soon became to be known as “The Universal”. This is because of something Mr. David’s refer to as technological Lock In, meaning acquiring standardization in its field. The reason for the QWERTY system became locked in, was because of the advent of an innovation called touch writing. This is a way of typing where the typist has learned the position of the letters, and has trained to use all fingers to tap the appropriate key, rather than the eagle method, where the fingers search and dive for each letter. This touch system was developed for many keyboards, but it was at its inception adapted for the Remington machine that used the QWERTY system. It quickly followed that if a person wanted to acquire a skill that was in demand, learning the QWERTY touch was a way to get a job. It also follows that when you have a workforce already skilled in using a certain touch system, it would be profitable in the short run to invest in machines (which where in the same price range anyway) rather than in acquiring new skills for the employees. W. Brian Arthur calls this “adoption”.[74] The theory states that when technologies

[74] ”Competing technologies, increasing returns, and lock in by historical events”, W. Brian Arthur, Nr.99, The economic journal, March 1989.

compete, one technology would sooner or later gain an advantage. When this adoption occurs, for whatever the reasons, it can lead to a technology being locked in, becoming a standard in its field. This again could explain why a technology that is clearly inferior of another technology, still can get the upper hand. One of the reasons for this might be what Mr. Arthur “initial advantage”. If a technology is first with an innovation, it could experience something called “increased returns”, meaning a situation where the technology gets more and more adoption by the actors in the field, thus creating momentum for the technology. If we apply this to the QWERTY system, we see that since this system was the first, therefore creating a market of both hardware and compatible software (Human resources), the probability is that the next actor that take to the field will chose this system, rather than a competing technology because of the cost effectiveness of the existing compatibility. If the actor where to chose the DSK, which was clearly a more superior technology, that would be more efficient in the long run, but the cost of implementation would be higher since the human resources most probably would have to be retrained to this system. Since there would be a lower implementation cost to chose the QWERTY system, because there would be a larger human resources pool to chose from, the chances are that actors would chose this, further increasing the returns to this technology and thus locking in the QWERTY technology. This would also create another situation, where future development in the field would be path dependent, meaning that once a technology has been locked in, further development would be constricted within the limits of the existing technology. An example of this could be the use of QWERTY keyboards for computers. A computer and its keyboard is a different technology from the typewriter, but the layout of the QWERTY system is still the same. As a curiosity worth mentioning, the Apple computer offers an electronic switch that would change the keyboard from QWERTY to DSK. (This

would also require the user to change the position of all the keys accordingly.) There is of course the possibility that the keyboard technology will disappear over time, being replaced by voice commands for computers, but as of yet, the keyboard is locked in with the QWERTY system.